

PCTWORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L	A2	(11) International Publication Number: WO 99/25086
		(43) International Publication Date: 20 May 1999 (20.05.99)

(21) International Application Number: PCT/FI98/00879

(22) International Filing Date: 11 November 1998 (11.11.98)

(30) Priority Data:
974198 11 November 1997 (11.11.97) FI(71) Applicant (for all designated States except US): SONERA OY
[FI/FI]; Sturenkatu 16, FIN-00510 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant (for US only): LAHTINEN, Pasi [FI/FI];
Aittatie 1 A 3, FIN-00390 Helsinki (FI).(74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A,
P.O. Box 981, FIN-00101 Helsinki (FI).(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR,
BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD,
GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR,
KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN,
MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK,
SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW,
ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW),
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR,
GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF,
BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN,
TD, TG).**Published***Without international search report and to be republished
upon receipt of that report.*

(54) Title: GENERATION OF A SEED NUMBER

(57) Abstract

Method for computing the key to an encryption algorithm used to encrypt messages to be transmitted over a telecommunication network and for generating the seed number needed for the computation of the encryption key. According to the invention, the seed number used is a number computed from a random number generated by the authentication centre of the mobile communication network, and the encryption key is computed using the authentication algorithm from the seed number and a subscriber identification key.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

GENERATION OF A SEED NUMBER

The present invention relates to a method as defined in the preamble of claim 1 for computing the key to an encryption algorithm used to encrypt messages transmitted over a telecommunication network and for generating the seed number needed for the computation of the encryption key by making use of the subscriber identity module of a mobile station. Moreover, the invention relates to a system as defined in the preamble of claim 7 for computing the key to an encryption algorithm used to encrypt messages transmitted over a telecommunication network and for generating the seed number needed for the computation of the encryption key by making use of the subscriber identity module of a mobile station.

In the near future, it is to be expected that further applications will be designed for mobile station subscriber identity modules, such as SIM cards (Subscriber Identity Module, SIM), in which encryption of communication is required. The encryption algorithm implementing the encryption needs an encryption key. In prior art, a method is known in which a separate algorithm for computing the encryption key is implemented in the subscriber identity module of a mobile station. In another prior-art method, the encryption key is stored on the subscriber identity module in conjunction with manufacture. In yet another previously known method, the encryption key is stored on the subscriber identity module when the latter is taken into use. A problem with the prior-art methods is that managing the seed number needed for the computation of the encryption key and/or managing the encryption key is difficult and, e.g. in solutions based on an RSA algorithm, separate equipment is needed. A further problem is that an encryption key permanently stored on the subscriber identity module is not as secure as an encryption key having a variable value.

The object of the present invention is to disclose a new type of method that eliminates the problems described above. A further object of the invention is to disclose a system that can be used to implement
5 said method.

A specific object of the present invention is to disclose a method and a system that allow flexible and safe management of seed numbers and encryption keys.

10 As for the features characteristic of the present invention, reference is made to the claims.

In the method of the invention, the encryption key required by the encryption algorithm used for the encryption of communication is computed from a certain
15 seed number by making use of the subscriber identity module of the mobile station. When the mobile station is activated, its subscriber identity module performs an authentication procedure with the mobile communication network. This is done by using an operator-specific authentication algorithm and a seed number
20 consisting of a random number RAND generated by the mobile communication network. The same authentication algorithm can be used to compute an encryption key. The seed number is a number computed on the basis of a random number RAND generated by the authentication centre
25 AC of the mobile communication network. Using the seed number and a subscriber identification key K_i as starting values for the authentication algorithm, an application in the subscriber identity module computes the
30 encryption key and stores it in the subscriber identity module. This encryption key is used when messages are to be encrypted and/or decrypted.

As compared with prior art, the present invention has the advantage that it makes the management of
35 seed numbers and encryption keys considerably easier and simpler than before. As the seed numbers and encryption keys are calculated in the subscriber identity module when necessary, they need not be transmitted or

set. A further advantage is that no separate equipment is needed for the management of seed numbers and encryption keys, which means that cost savings are achieved. The invention also increases security. In the method of the invention, the encryption key changes continuously and it is not transmitted anywhere, thus considerably reducing the chance of its getting into the hands of outsiders.

In an embodiment of the method, a seed number is calculated from a random number RAND generated by the authentication centre, producing a seed number such as $RAND+1$.

In an embodiment of the method, the encryption key is computed by using an A3 algorithm, which is an operator-specific authentication algorithm.

In an embodiment of the method, one or more encryption keys are used. In this case, each application requiring encryption has its own encryption key, thus increasing security.

In an embodiment of the method, the encryption key is computed by using one or more successive algorithms so that the result of the preceding algorithm is used as the seed number for the next algorithm. This provides the advantage that the seed number for the new algorithm is changed, which leads to increased security.

In an embodiment of the method, a certain portion of the random number range used by the mobile communication network is reserved for the calculation of seed numbers.

The system of the invention for computing the key to an encryption algorithm used to encrypt messages transmitted over a telecommunication network and for generating the seed number needed for the computation of the encryption key by making use of the subscriber identity module of a mobile station comprises an encryption device and means for the transmission of encrypted messages. The encryption device comprises a me-

ans for computing an encryption key from a seed number. The means used to transmit encrypted messages comprise a mobile station and an encryption server.

5 In an embodiment of the system, an encryption device is implemented both in the subscriber identity module and in the authentication centre.

In an embodiment of the system, the encryption device comprises a device for storing the encryption key.

10 In an embodiment of the system, the mobile station is GSM compatible.

In the following, the invention will be described by the aid of an embodiment example by referring to the attached drawings, wherein

15 Fig. 1a and 1b illustrate an example representing the method of the invention in the form of logic diagrams; and

Fig. 2 presents an example representing the hardware configuration of the system of the invention.

20 Fig. 1a illustrates a method in which the mobile communication network generates a random number RAND and sends it to the subscriber identity module 9. Based on this random number, a seed number RAND+1 is calculated. This seed number 1 and the identification
25 key K_i 2 are input as starting values to an A3 algorithm 3. The identification key K_i 2 is a user-specific secret parameter, which has been stored in the subscriber identity module 9 and in the authentication centre 10. The A3 algorithm 3 is the same operator-specific
30 algorithm that is used when the subscriber identity module 9 carries out an authentication procedure with the authentication centre 10 of the mobile communication network upon activation of the mobile station 8. A feature characteristic of the A3 algorithm 3 is that com-
35 puting the encryption key 4 from the seed number 1 and the identification key K_i 2 is easy, but determining the identification key 2 on the basis of the seed number 1 and the encryption key 4 is extremely difficult.

The encryption key 4 is the result produced by the algorithm 3. This encryption key 4 is used when messages are to be encrypted and/or decrypted.

Fig. 1b illustrates a variation of the method of the previous example. In this case, it is assumed that the random number range is 0 - 10000. It is divided into two halves so that the random number RAND values 0 - 4999 are reserved for the computation of seed numbers 5. the mobile communication network generates a random number RAND and sends it to the subscriber identity module 9. Based on the random number, a seed number $RAND+5000$ is calculated. The seed number 5 and the identification key K_i 2 are input as starting values to the A3 algorithm 3, which produces a new seed number 6 as a result. The new seed number 6 thus computed and the identification key K_i 2 are given as starting values to a new algorithm 7. The result obtained is used as the final encryption key 4. The advantage provided by this alternative is that the seed number 6 for the new algorithm 7 is automatically changed.

Fig. 2 illustrates a system in which encrypted short messages are transmitted between a GSM telephone 8 and an encryption server 12 in a GSM network. An encryption device 11 has been implemented both in the subscriber identity module 9 of the mobile station 8 and in the authentication 10 of the GSM network. The encryption device 11 comprises a SIM Application Toolkit, an application that computes the encryption key 4. In addition, the encryption device 11 stores the computed encryption key 4 for use. When messages to be encrypted and/or decrypted are transmitted, the encryption device 11 computes an encryption key 4 on the basis of a seed number 1 and a user-specific identification key K_i 2 both on the SIM card 9 and in the authentication centre 10. Based on this encryption key 4, an encryption algorithm, such as an RSA or 3DES algorithm, implemented both on the SIM card and in the authentication server 12, encrypts/decrypts the message. The key

4 is stored for the next time it is needed, or a new value for the key is computed each time.

The invention is not restricted to the examples of its embodiments described above, but many variations are possible within the scope of the inventive idea defined by the claims.

5

CLAIMS

1. Method for computing the key (4) to an encryption algorithm used to encrypt messages to be transmitted over a telecommunication network and for
5 generating the seed number (1, 5) needed for the computation of the encryption key (4) by making use of the subscriber identity module (9) of a mobile station (8), in which method the key to the encryption algorithm is computed from the seed number (1, 5) using a certain
10 algorithm (3, 7), characterised in that

- the seed number (1, 5) used is a number computed from a random number RAND generated by the authentication centre (AC) (19) of the mobile communication network; and

15 - using the authentication algorithm (3) of the mobile communication network, the encryption key (4) required by the encryption algorithm is computed from the seed number (1, 5) and a subscriber identification key K_i (2).

20 2. Method as defined in claim 1, characterised in that the seed number is calculated from the random number RAND generated by the authentication centre (10), producing a seed number such as $RAND+1$.

25 3. Method as defined in claim 1 or 2, characterised in that the encryption key (4) is computed by using an A3 algorithm (3).

4. Method as defined in any one of claims 1 - 3, characterised in that one or more encryption keys are used.

30 5. Method as defined in any one of claims 1 - 4, characterised in that the encryption key is computed by using one or more successive algorithms (3, 7) in such manner that the result of the preceding algorithm (3) is used as the seed number for the next
35 algorithm (7).

6. Method as defined in any one of claims 1 - 5, characterised in that a certain portion of

the random number range used by the mobile communication network is reserved for the computation of seed numbers (1, 5).

5 7. System for computing the key (4) to an encryption algorithm used to encrypt messages to be transmitted over a telecommunication network and for generating the seed number (1, 5) needed for the computation of the encryption key by making use of the subscriber identity module (9) of a mobile station (8),
10 said system comprising an encryption device (11) and means (8, 12) for the transmission of encrypted messages, characterised in that

- the encryption device (11) comprises a means for computing the encryption key (4) from the seed number (1, 5); and
15

- the means used to transmit encrypted messages comprise a mobile station (8) and an encryption server (12).

20 8. System as defined in claim 7, characterised in that an encryption device (11) is implemented both in the subscriber identity module (9) and in the authentication centre (10).

25 9. System as defined in claim 7 or 8, characterised in that the encryption device (11) comprises a device for storing the encryption key (4).

10. System as defined in any one of claims 7 - 9, characterised in that the mobile station (8) is GSM compatible.

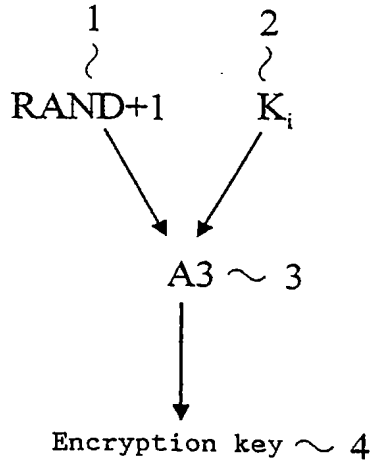


Fig. 1a

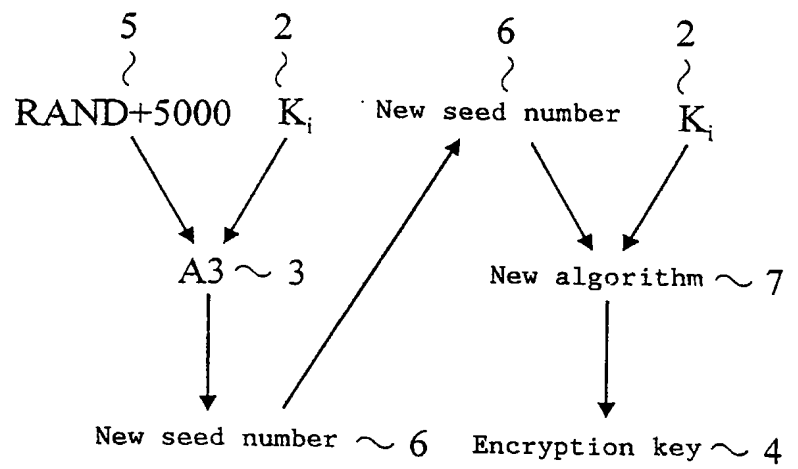


Fig. 1b

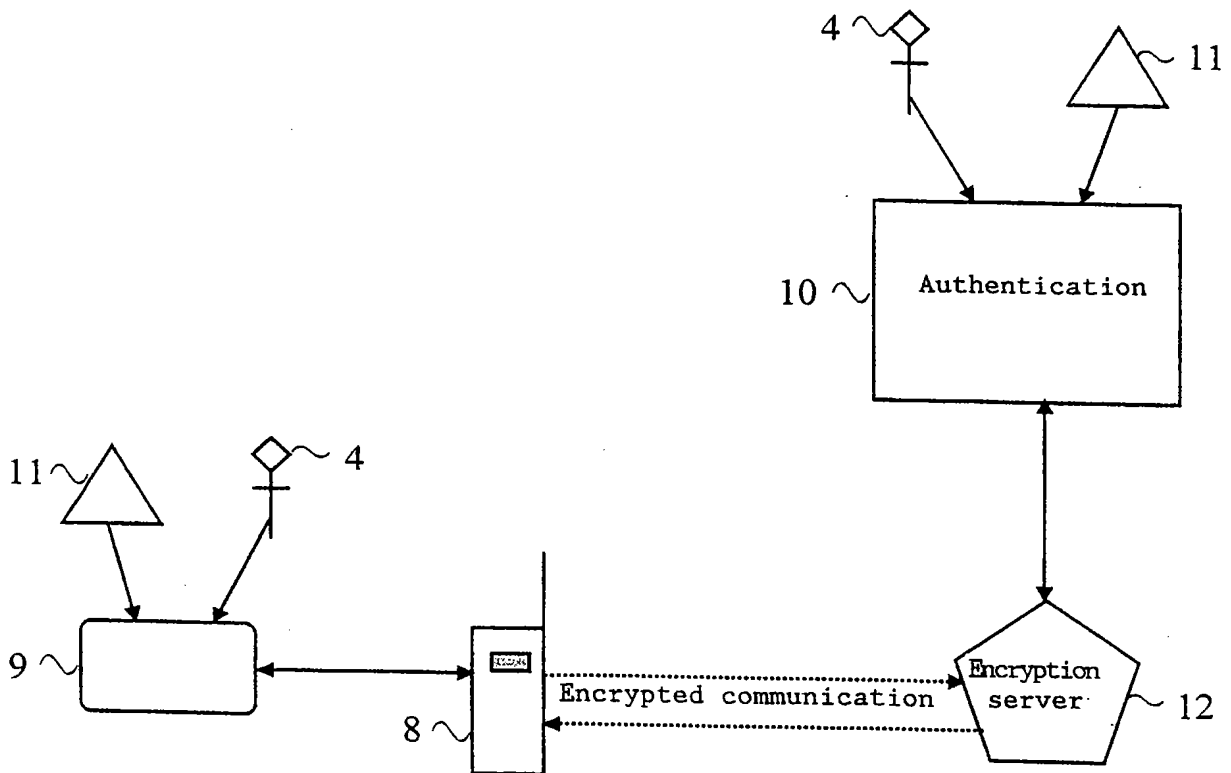


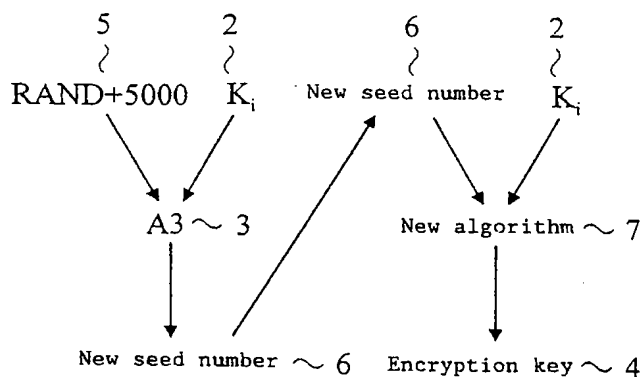
Fig. 2



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04Q 7/38, H04L 9/30		A3	(11) International Publication Number: WO 99/25086
			(43) International Publication Date: 20 May 1999 (20.05.99)
(21) International Application Number: PCT/FI98/00879		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 11 November 1998 (11.11.98)			
(30) Priority Data: 974198 11 November 1997 (11.11.97) FI			
(71) Applicant (for all designated States except US): SONERA OY [FI/FI]; Sturenkatu 16, FIN-00510 Helsinki (FI).			
(72) Inventor; and			
(75) Inventor/Applicant (for US only): LAHTINEN, Pasi [FI/FI]; Aittatie 1 A 3, FIN-00390 Helsinki (FI).		Published With international search report.	
(74) Agent: PAPULA REIN LAHTELA OY; Fredrikinkatu 61 A, P.O. Box 981, FIN-00101 Helsinki (FI).		(88) Date of publication of the international search report: 28 October 1999 (28.10. 99)	

(54) Title: GENERATION OF A SEED NUMBER



(57) Abstract

Method for computing the key to an encryption algorithm used to encrypt messages to be transmitted over a telecommunication network and for generating the seed number needed for the computation of the encryption key. According to the invention, the seed number used is a number computed from a random number generated by the authentication centre of the mobile communication network, and the encryption key is computed using the authentication algorithm from the seed number and a subscriber identification key.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon	KR	Republic of Korea	PL	Poland		
CN	China	KZ	Kazakhstan	PT	Portugal		
CU	Cuba	LC	Saint Lucia	RO	Romania		
CZ	Czech Republic	LI	Liechtenstein	RU	Russian Federation		
DE	Germany	LK	Sri Lanka	SD	Sudan		
DK	Denmark	LR	Liberia	SE	Sweden		
EE	Estonia			SG	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 98/00879

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04Q 7/38, H04L 9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04Q, H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	M. Mouly, M.B. Pautet: The GSM System for Mobile Communications, France 1992; sections 7.2.2 & 7.2.3	1,3,6-10
Y	--	2,4,5
Y	US 5590200 A (J.B. NACHMAN ET AL), 31 December 1996 (31.12.96), figures 2-6, abstract	2,4,5
A	--	1,3,6-10
A	EP 0688929 A2 (NANOTEQ (PROPRIETARY) LIMITED), 27 December 1995 (27.12.95), column 28, line 47 - column 29, line 3, figure 4a	2,4,5
	--	

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

26 July 1999

Date of mailing of the international search report

04 August 1999 (04.08.99)

Name and mailing address of the ISA/

Swedish Patent Office

Box 5055, S-102 42 STOCKHOLM

Facsimile No. +46 8 666 02 86

Authorized officer

Per Källquist/MN

Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

International application No.

PCT/FI 98/00879

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5144665 A (K. TAKARAGI ET AL), 1 Sept 1992 (01.09.92), column 18, line 67 - column 19, line 3, figure 5 --	2,4,5
A	US 5201000 A (S.M. MATAYAS ET AL), 6 April 1993 (06.04.93), column 17, line 48 - column 18, line 30, figures 10,11 --	2,4,5
A	US 4797672 A (P.T. KOUSA), 10 January 1989 (10.01.89), column 2, line 3 - line 10; column 4, line 54 - line 61; column 4, line 66 - column 5, line 4, column 6, line 41 - line 44 --	2,4,5
A	WO 9712461 A1 (TELEFONAKTIEBOLAGET LM ERICSSON), 3 April 1997 (03.04.97), page 7, line 4 - page 8, line 4, figure 3, abstract -- -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

01/07/99

International application No.

PCT/FI 98/00879

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5590200 A	31/12/96	AT 171331 T AU 684112 B AU 8034294 A CA 2137608 A DE 69413361 D EP 0658054 A,B IL 107967 A JP 7288522 A	15/10/98 04/12/97 15/06/95 10/06/95 00/00/00 14/06/95 05/12/96 31/10/95
EP 0688929 A2	27/12/95	US 5686904 A ZA 9505429 A	11/11/97 13/02/96
US 5144665 A	01/09/92	JP 3243035 A	30/10/91
US 5201000 A	06/04/93	CA 2075254 A EP 0534420 A JP 2690004 B JP 5224604 A	28/03/93 31/03/93 10/12/97 03/09/93
US 4797672 A	10/01/89	NONE	
WO 9712461 A1	03/04/97	AU 7102196 A CA 2233463 A CN 1198278 A EP 0872078 A SE 506619 C SE 9503343 A	17/04/97 03/04/97 04/11/98 21/10/98 19/01/98 28/03/97